PB82-177767

TSCA (Toxic Substances Control Act) Confidential Business Information Security Manual: Revised

(U.S.) Environmental Protection Agency
Washington, DC

Oct 81

U.S. Department of Commerce
National Technical Information Service
NTIS.

EPA-560/1-82-001

PB82-177767

TSCA CONFIDENTIAL BUSINESS INFORMATION SECURITY MANUAL

October 1981

United States Environmental Protection Agency
Washington, D.C. 20460

REPRODUCED BY
NATIONAL TECHNICAL
INFORMATION SERVICE
U.S. DEPARTMENT OF COMMERCE
SPRINGFIELD, VA 22161

BIBLIOGRAPHIC INFORMATION

PB82-177767

TSCA (Toxic Substances Control Act) Confidential Business Information Security Manual; Revised.

Oct 81

PERFORMER: Environmental Protection Agency, Washington, DC. Office of Toxic Substances.

These procedures prescribe minimum standards and establish responsibility and accountability for the control of documents and computer systems that contain confidential business information (CBI) received by EPA under the Toxic Substances Control Act (TSCA).

KEYWORDS: *Contractors, *Data processing security, *Computer information security, *Confidentiality.

Available from the National Technical Information Service, Springfield, Va. 22161

PRICE CODE: PC A04/MF A01

Preface

This revised *TSCA Confidential Business Information Security Manual* deals with a serious and continuing obligation we at EPA have under the Toxic Substances Control Act (TSCA)--the need to protect confidential business information from unauthorized disclosure.

TSCA requires industry to entrust large amounts of data to EPA concerning the tens of thousands of chemical substances in U.S. commerce. This information has never been compiled in such a complete way before, and it forms the basis for our ability to carry out TSCA's preventive approach to minimizing the health and environmental risks of toxic chemicals.

Some of these industry data are claimed as "confidential," meaning that they involve trade secrets or other kinds of information that one company doesn't want another to have. Understandably, industry has expressed great concern about EPA's ability to protect confidential business information from unauthorized disclosure.

For the past 2 years, TSCA Confidential Business Information has been protected under procedures in the *TSCA Confidential Business Information Security Manual*. The EPA Data Security Task Force has developed this revised Manual after considering suggestions and comments from throughout the Agency and from the public. I believe that this Manual properly balances the need for data security with our requirements for access to the data.

Any security system is only as good as the people who maintain it. Only by all of us working together can it succeed, but any one of us acting carelessly or negligently could cause us to fail. I urge you to study and learn these procedures and to encourage those you work with to do the same. While I don't wish to overemphasize this point, TSCA provides strict criminal penalties for any person who discloses this confidential business information in a knowing and unauthorized way, and we have gone on public record with the promise to prosecute any acts of wrongful disclosure to the fullest extent of the law.

These procedures provide the kind of protection we at EPA must offer in order to continue to have the information we need to carry out TSCA. We are counting on you to make this system work.

July 29, 1981
Date

Warren R. Muir
Deputy Assistant Administrator
for Toxic Substances

Contents

		Page
PREFACE		iii
GLOSSARY OF ACRONYMS		ix
I.	GENERAL	1
	A. Purpose	1
	B. Policy	1
	C. Applicable Federal Statutes and Regulations	1
	D. Authority	1
	E. Treatment of Violations	1
	F. Maintenance of Discipline	2
	G. Authorization for Access to TSCA CBI	2
	H. Definitions	4
	I. Forms	6
	J. Security Procedures for Individual EPA Offices	6
	K. Contractor Security Requirements	6
II.	RESPONSIBILITIES	7
	A. Assistant Administrator for Pesticides and Toxic Substances (AA/OPTS)	7
	B. Deputy Assistant Administrator for Toxic Substances (DAA/OTS)	7
	C. Office of the Inspector General (OIG)	7
	D. Division Directors	8
	E. Director, Management Information and Data Systems Division (MIDSD)	8
	F. Branch Chiefs	8
	G. Chief, Information Control Branch (ICB)	9
	H. Chief, Security Branch, Facilities and Support Services Division (FSSD)	9
	I. Document Control Officers	9
	J. Document Control Officers (and Document Control Assistants) Approved for Computer Access	10
	K. Computer DCOs	10
	L. Document Control Assistants	11
	M. EPA Employees	11
	N. Security Representatives	11
III.	PROCEDURES FOR HANDLING TSCA CONFIDENTIAL BUSINESS INFORMATION	13
	A. Gaining Access	13
	B. Storage	13
	C. Safeguards During Use	14
	D. Transmittal	17
	E. Reproduction/Destruction	17
	F. Photographs	18

Contents (cont.)

Page

G. Retiring of Documents 18
H. Generating TSCA Confidential Business Information Documents 18
I. Retaining Logs 18

IV. SECURITY REQUIREMENTS FOR EPA COMPUTER CENTERS 19
A. General 19
B. Hardware and Software Characteristics 19
C. Media Handling 22
D. Facility Protection 23
E. Backup and Recovery Capability 23

V. SECURITY REQUIREMENTS FOR OTHER FEDERAL AGENCIES 25
A. Purpose 25
B. Policy 25
C. Procedures for Answering Requests 25
D. Procedures for Interagency Agreements 26
E. Exemption for the Department of Justice 26
F. Limited Access 27
G. Violations 27

APPENDIX I EXCERPTS FROM *EPA CONDUCT AND DISCIPLINE MANUAL* 29

APPENDIX II INVENTORY LOG 32

APPENDIX III USER SIGN-OUT LOG 33

APPENDIX IV DESTRUCTION LOG 34

APPENDIX V CONTRACTOR/SUBCONTRACTOR SIGN-OUT LOG 35

APPENDIX VI FEDERAL AGENCY, CONGRESS, AND FEDERAL COURT SIGN-OUT LOG 36

APPENDIX VII TSCA FEDERAL NON-EPA EMPLOYEE CONFIDENTIALITY AGREEMENT 37

APPENDIX VIII CONFIDENTIALITY AGREEMENT FOR UNITED STATES EMPLOYEES UPON TERMINATION OR TRANSFER 38

APPENDIX IX TSCA CBI COVER SHEET 39

Contents (cont.)

		Page
APPENDIX X	AUTHORIZATION FOR ACCESS TO TSCA CBI	40
APPENDIX Xa	REQUEST FOR APPROVAL OF TEMPORARY EMPLOYEE, FOR ACCESS TO TSCA CBI	41
APPENDIX XI	LOAN RECEIPT FOR TSCA CBI	42
APPENDIX XII	TSCA CBI MEETING SIGN-IN SHEET	43
INDEX		45

Glossary of Acronyms

AA/OPTS	Assistant Administrator for Pesticides and Toxic Substances
ADP	Automated Data Processing
CBI	Confidential Business Information
CFR	*Code of Federal Regulations*
DAA/OTS	Deputy Assistant Administrator for Toxic Substances
DCA	Document Control Assistant
DCO	Document Control Officer
DOJ	Department of Justice
EPA	United States Environmental Protection Agency
FSSD	Facilities and Support Services Division
IAG	Interagency Agreement
ICB	Information Control Branch
MIDSD	Management Information and Data Systems Division
NACI	National Agency Check and Inquiries
OGC	Office of General Counsel
OIG	Office of the Inspector General
OPTS	Office of Pesticides and Toxic Substances
OTS	Office of Toxic Substances
TSCA	Toxic Substances Control Act

I. General

A. Purpose

These procedures prescribe minimum standards and establish responsibility and accountability for the control of documents and computer systems that contain confidential business information (CBI) received by EPA under the Toxic Substances Control Act (TSCA) (15 U.S.C. § 2601 et seq.).

B. Policy

EPA recognizes its responsibility to the submitters of CBI. All reasonable measures must be taken to prevent the unauthorized disclosure of CBI. EPA employees are prohibited from disclosing, in any manner or to any extent not authorized by law or EPA regulations, any TSCA CBI they have access to in the course of their employment or official duties. Employees of other Federal agencies are also prohibited from disclosing, in any manner or to any extent not authorized by law or the terms of an agreement between EPA and the other agency, any TSCA CBI released to them by EPA. TSCA CBI is to be held in confidence and always handled in accordance with these procedures.

C. Applicable Federal Statutes and Regulations

- 15 U.S.C. § 2613, Disclosure of Data (TSCA).
- 5 U.S.C. § 552, Freedom of Information Act.
- 40 CFR Part 2, Confidentiality of Business Information.
- 41 CFR Chapter 15, Public Contracts and Property Management.

D. Authority

The Assistant Administrator for Pesticides and Toxic Substances (AA/OPTS) is charged with the responsibility to design and implement an Agencywide security program to control the receipt, handling, and dissemination of TSCA CBI. Requirements promulgated under this authority shall supplement, but not supersede, the general Agency regulations pertaining to Freedom of Information requests and confidentiality as set forth in 40 CFR Part 2.

E. Treatment of Violations

Unauthorized disclosure of TSCA CBI may subject an employee to criminal penalties under TSCA § 14(d)(1) as follows:

> Criminal Penalty for Wrongful Disclosure--(1) Any officer or employee of the United States or former officer or employee of the United States, who by virtue of such employment or official position has obtained possession of, or has access to, material the disclosure of which is prohibited by subsection (a), and who knowing that disclosure of such material is prohibited by such subsection, willfully discloses the material in any manner to any person not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000 or imprisoned for not more than one year, or both.

Also, violations of these procedures by employees may result in removal from the TSCA CBI Authorized Access List and disciplinary action with penalties up to and including dismissal, under procedures detailed in the *EPA Conduct and Discipline Manual* [Chapter 5 and Appendix C, Table of Offenses and Penalties, 35 (b)].

F. Maintenance of Discipline

If a security system is to operate successfully, discipline must be maintained among employees. Chapter 5 and Appendix C of the *EPA Conduct and Discipline Manual* deal with this subject in depth. All employees, and especially supervisors, shall become thoroughly familiar with that material. Pertinent excerpts from Chapter 5 and Appendix C of the *EPA Conduct and Discipline Manual* are included in Appendix I of this Manual.

An informal corrective action, not mentioned in the *EPA Conduct and Discipline Manual*, that can be taken by supervisors at the Division Director level and above, is removal from the TSCA CBI Authorized Access List. This action will communicate to the employee the seriousness of his/her actions and also prevent further violations or possible unauthorized disclosures of TSCA CBI. Although removal from the Authorized Access List is an informal measure, it is a serious measure and shall be used judiciously. If an employee is removed from the list it is important to notify coworkers and the Chief, Information Control Branch (ICB), promptly to be sure all further access to CBI is denied.

G. Authorization for Access to TSCA CBI

1. *Applying for Authorization*

When an employee requires access to TSCA CBI, the following steps must be taken to apply for inclusion on the TSCA CBI Authorized Access List.

The employee must sign section III of the authorization form (Confidentiality Agreement for EPA Employees).

Section 1 of the Authorization for Access to TSCA Confidential Business Information (CBI) form must be completed and signed by the appropriate authorizing official (see Appendix X). Authorizing officials must be equivalent to a supervising Division Director or above and may only authorize those employees

under their supervision. In facilities where there is no Document Control Officer (DCO)/Document Control Assistant (DCA), the authorizing official must also sign section IV of the authorization form. (Cross out "Local DCO/DCA" and insert proper title.)

If the employee is being appointed as a DCO/DCA, the authorizing official (Division Director at Headquarters, Regional Administrator or Laboratory Director in the field) must also sign section II of the authorization form.

The authorization form shall be taken to the local DCO or DCA who will certify by signing and dating section IV that all necessary forms have been completed and forwarded to the Security Branch, EPA Headquarters. (For all employees except those described in section G.3. below under "exceptions," and those who require full field investigations, the local DCO/DCA may assume that the proper forms were completed at the time of employment.) The local DCO/DCA will keep the original of the authorization form for his/her files and send a copy within 10 days to the Chief, ICB.

Upon completion of these steps, the local DCO/DCA will place the employee's name on the Authorized Access List and notify the employee.

Summer employees of 4 months or less and temporary or seasonal employees limited to 3 months are not to be processed for access to TSCA CBI without written authorization of the Chief, Information Control Branch. Division Directors (or equivalent) must submit a Request for Approval of Temporary Employee for Access to TSCA/CBI (see Appendix Xa) prior to submission of the required investigative forms to the Information Control Branch.

2. *Keeping the Authorized Access List Current*

The Authorized Access List must be kept current. On the first working day of each month, every DCO/DCA in EPA will send a corrected, updated copy of his particular Authorized Access List to the Chief, ICB. Using these updated lists, a master TSCA CBI Access List will be compiled and distributed.

When an employee who has had access to TSCA CBI terminates or transfers to a position not requiring access to TSCA CBI, he/she must be processed through the local DCO/DCA to ensure that all TSCA CBI documents have been returned and to sign the Confidentiality Agreement for United States Employees Upon Termination or Transfer (Appendix VIII). This agreement will be kept on file by the local DCO/DCA for 5 years. The local DCO/DCA will immediately delete the terminated or transferred employee's name from the Authorized Access List and will ensure that this deletion is reflected in the next monthly list sent to the Chief, ICB.

3. *Background Investigation and Related Forms*

All employees who will have access to TSCA CBI must be investigated. All those with permanent appointments or those with temporary appointments of 700 hours or more per annum must complete investigation forms at the time they are employed. At that time a National Agency Check and Inquiries (NACI) investigation is automatically initiated. Division Directors may authorize access to TSCA CBI for these employees, once their need for access has been established.

Exceptions to this rule include consultants, who may be authorized access but must first complete and submit certain required forms--SF-171, Personal Qualifications Statement; SF-85, Data for Nonsensitive or Noncritical-Sensitive Position; and SF-87, United States Civil Service Commission Fingerprint Chart--for initiation of an NACI. These forms must be submitted to the EPA Headquarters Security Branch prior to such authorization.

Document Control Officers and Assistants and others designated by the Chief, Information Control Branch must have a Full Field Investigation. The authorizing official will ensure all the completion of necessary forms. SF-87, United States Civil Service Commission Fingerprint Chart, CSC Form 329-A, Authority for Release of Information, and EPA Form 1480-29, Personal History Statement for Administrative Full Field Position, are necessary for the initiation of such an investigation and must be submitted to the EPA Headquarters Security Branch along with a copy of the completed Authorization for Access form, prior to the assumption of duties.

Any information developed during a background investigation that reflects adversely on an employee's suitability or trustworthiness in handling TSCA CBI will be referred to the Chief, Security Branch, by the agency conducting the investigation. After completion of actions required by Part II (Personnel Security) Chapter 3 (Handling of Security Cases), EPA Security Manual, dated 1/6/81, if appropriate, the Chief, Security Branch, will notify the Chief, Information Control Branch, of the results of such actions.

H. Definitions

Access is the ability and opportunity to gain knowledge of confidential business information (in any manner whatsoever).

The *ADP Application Security Plan* is a formal, documented plan that addresses the administrative, technical, and physical controls required during each phase in the life cycle of an application system processing TSCA CBI.

An *Authorized Computer Facility* is an EPA or contractor computer facility that meets the security standards contained in Chapter IV of this Manual and that has been approved, in accordance with Chapter II, for handling TSCA CBI.

An *Authorized Person* is any person who is authorized, in accordance with the requirements of Chapter III, for access to TSCA CBI.

The *Computer Center Security Plan* is a formal, documented plan that addresses the administrative, technical, and physical controls required to protect TSCA CBI within the data center.

Computer Direct-Access Authorization is a special authorization issued, upon approval by the Deputy Assistant Administrator for Toxic Substances (DAA/OTS), to an authorized person by the appropriate Division Director for direct access to computerized TSCA CBI.

A *Computer Document Control Officer* is a Document Control Officer (DCO) within a computer facility responsible for the security and control of TSCA Confidential Business Information contained in the computer facility.

Confidential Business Information is any information in any form received by EPA or an EPA contractor from any person, firm, partnership, corporation, or association; local, State, or Federal agency; or foreign government that contains trade secrets or commercial or financial information, that has been claimed as confidential by the person submitting it, and that has not been determined to be nonconfidential under the procedures in 40 CFR Part 2.

A *Document* is any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing card decks, printouts, and tapes; maps and charts; paintings; photographs; drawings; engravings; sketches; samples; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

A *Document Control Assistant (DCA)* is a person who is responsible for assisting the Document Control Officer in performing duties related to information processing, document control, and security.

A *Document Control Number* is the unique number assigned by a Document Control Officer or through computer system numbering to a document containing TSCA CBI.

A *Document Control Officer (DCO)* is a person designated, in accordance with Chapter II, to be responsible for the security, control, and distribution of all TSCA CBI received by him/her.

An *Employee* is any person employed by the U.S. Environmental Protection Agency, including EPA Administrative Law Judges, on a full-time or part-time basis in accordance with the procedures of the Office of Personnel Management. This definition does not include contractors, grantees, or their employees.

A *Federal Agency* is any organization or entity composed of United States officers or employees except for Federal courts and Congress.

Information is knowledge that can be communicated by any means.

A *Secure Facility* is a building or portion of a building that meets the requirements of this Manual for handling TSCA CBI and has been approved by the Information Control Branch (ICB).

A *Secure Room* or area is a room or area which meets the requirements of this Manual for storage and/or use of TSCA CBI and which has been approved by the ICB.

A *Security Representative* is an authorized person designated by the Regional Administrator or Laboratory Director, and approved by the Security Branch, to establish and maintain adequate safeguards for the protection of personnel, property, and data. This individual is the liaison on all security matters between the EPA Headquarters Security Branch and his/her Region or Laboratory.

A *Submitter Representative* is an authorized representative of a company who may be permitted to review his company's own TSCA CBI submissions.

A *Violation* is the failure to comply with any provision in these procedures, whether or not such failure leads to actual unauthorized disclosure of TSCA CBI.

I. Forms

The forms required for the implementation of these procedures include five basic logs: the Inventory Log (Appendix II), the User Sign-Out Log (Appendix III), the Destruction Log (Appendix IV), the Contractor/Subcontractor Sign-Out Log (Appendix V), the Federal Agency, Congress, and Federal Court Sign-Out Log (Appendix VI). Individual offices may design different logging systems to meet their specific needs; however, such logs must contain, at a minimum, the information in the basic logs.

Other forms used in implementing these procedures are:

- TSCA Federal Non-EPA Employee Confidentiality Agreement (Appendix VII).
- Confidentiality Agreement for United States Employees Upon Termination or Transfer (Appendix VIII).
- TSCA Confidential Business Information Cover Sheet (Appendix IX).
- Authorization for Access to TSCA Confidential Business Information (Appendix X).
- Loan Receipt for TSCA Confidential Business Information (Appendix XI).
- TSCA Confidential Business Information Meeting Sign-In Sheet (Appendix XII).

J. Security Procedures for Individual EPA Offices

Within EPA, program offices, Regions, and Laboratories may develop security procedures to meet their individual needs. Such procedures must meet the minimum standards contained in this *TSCA Confidential Business Information Security Manual* and be approved by the Chief, Information Control Branch. Upon request, the Information Control Branch and the OIG will advise and assist offices in the development of such procedures.

This policy does not apply to computer security procedures; individual offices may not develop their own computer security procedures.

K. Contractor Security Requirements

Security procedures for contractors and subcontractors are contained in a separate document, *Contractor Requirements for the Control and Security of TSCA Confidential Business Information*, which also includes the procedures for solicitation and award of contracts (or modification of existing contracts) that involve receipt or handling of TSCA CBI.

II. Responsibilities

A. Assistant Administrator for Pesticides and Toxic Substances (AA/OPTS)

The AA/OPTS is responsible for the overall implementation of these procedures and for approving other Federal agencies for access to TSCA CBI.

B. Deputy Assistant Administrator for Toxic Substances (AA/OTS)

The DAA/OTS is responsible for approving: Computer Center Security Plans for any computer facility that will receive TSCA CBI; ADP Application Security Plans prepared by software development managers, changes to this manual, when appropriate, and all computer DCO's and DCA's.

C. Office of the Inspector General (OIG)

The OIG is responsible for inspecting TSCA CBI operations, ensuring that they conform to procedures specified in this Manual, and conducting inspections when appropriate. To carry out these responsibilities, personnel from the OIG:

- Investigate cases of alleged or actual wrongful disclosure of CBI. Disclosures found to have been knowingly and willfully made will be referred to the Department of Justice, as appropriate.

- As appropriate, upon request of a Division Director, investigate violations of these procedures when disclosure was improper but not wrongful under TSCA §14(d)(1), the OIG will furnish the results of the investigation to the DAA/OTS for remedial and/or disciplinary action.

- As appropriate, investigate cases of alleged or actual wrongful disclosures of TSCA CBI in connection with interagency agreements (IAGs) developed under Chapter V of this Manual.

- Conduct initial inspections, when necessary, of Headquarters, Regional, and Laboratory facilities for compliance with security requirements in this Manual and forward appropriate reports to the ICB.

- Conduct reviews of security procedures at other Federal agencies and inspect their security facilities, prior to transfer of any TSCA CBI, to ensure compliance with the security provisions of IAGs.

- Conduct periodic inspections, announced and unannounced, of EPA offices or Laboratories to ensure continued compliance with the TSCA CBI security procedures.

D. Division Directors (or Equivalent)

Division Directors (or equivalent) are responsible for the implementation of these procedures in their areas of responsibility. Their responsibilities include appointing DCOs and DCAs as needed. The number of DCOs and DCAs shall be kept to a minimum. Only at EPA Headquarters may Division Directors appoint DCOs and DCAs. In Regional Offices and Laboratories this responsibility rests with Regional Administrators and Laboratory Directors and may not be delegated to a lower level.

Division Directors are also responsible for authorizing their employees for access to TSCA CBI. Access must be strictly on a need-to-know basis and the number of authorized persons must be kept to a practical minimum. Division Directors may also remove names of their employees from the access list.

Division Directors must request computer access to TSCA CBI from the DAA/OTS for their employees, including DCOs and DCAs.

Additional duties of Division Directors are to ensure that authorized persons participate in training and education programs, as available, regarding the handling of TSCA CBI; to take appropriate disciplinary action when any employee fails to comply with these procedures and to notify the DAA/OTS of the violation and any disciplinary action taken; to refer cases to the OIG when there is an alleged or actual wrongful disclosure of TSCA CBI; and to approve all requests for TSCA CBI that involve movement of documents from one EPA facility to another.

E. Director, Management Information and Data Systems Division (MIDSD)

The Director of the Management Information and Data Systems Division (MIDSD) will, upon request, assist the OIG in reviewing Computer Center Security Plans as specified in Chapter IV; review and comment on ADP Application Security Plans as specified in Chapter IV, and recommend approval or disapproval to the DAA/OTS; and assist the OIG in conducting inspections of computer facilities for compliance with security requirements.

F. Branch Chiefs

Branch Chiefs are responsible for the implementation of these procedures in their areas of responsibility. They or their designees are responsible for reviewing staff-generated documents in final form when there is a question as to whether or not these documents contain TSCA CBI. All staff-generated documents that are determined by the Branch Chief to contain TSCA CBI shall be taken immediately to the document control officer to be entered into the document control system.

Similarly, any sanitizing of staff-generated documents must be done by the Branch Chief or his/her designee.

If necessary, the Branch Chief shall consult the Chief, Information Control Branch, before making a decision.

G. Chief, Information Control Branch (ICB)

The Chief, Information Control Branch, is responsible for developing EPA policy in security matters within the framework of these procedures and 40 CFR Part 2. Responsibilities include interpreting, and/or clarifying, these procedures as needed to facilitate their implementation and serving as a consultant to all DCOs/DCAs regarding these procedures and any other matters relating to the control and security of CBI.

The Chief, Information Control Branch, also maintains current lists of DCOs and DCAs throughout EPA, all persons authorized for access to TSCA CBI throughout EPA, and all DCOs, DCAs, and other employees with computer access authorization.

The Chief, ICB, will also be responsible for approving Headquarters, Regional, and Laboratory facilities for receipt and storage of TSCA based on an Inspector General's report of inspection of these facilities for compliance with security requirements of this Manual.

The Chief, ICB, is responsible for recommending approval/disapproval of security procedures and facilities of other Federal agencies to the AA/OPTS.

H. Chief, Security Branch, Facilities and Support Services Division

The Chief, Security Branch, is responsible for assisting OPTS in establishing appropriate security measures to comply with the requirements of this Manual. He/she is responsible for ensuring that NACIs or full field investigations are conducted on employees, as appropriate.

The Chief, Security Branch, also assists various programs handling TSCA CBI in establishing the physical security for their particular operation, e.g., locks, electronic alarms, storage cabinets, shredders, etc.

I. Document Control Officers (DCOs)

All DCOs are responsible for the control and security of TSCA CBI received by them. They are responsible for logging all TSCA CBI received and generated, including computer-generated printouts, and assigning a document control number, attaching a cover sheet, and, at a minimum, stamping the first page and the back of the last page of all TSCA CBI documents, whenever these things have not already been done. All TSCA CBI logs must be marked and treated as CBI.

DCOs furnish TSCA CBI to other Federal agencies that are authorized to receive the information by the Assistant Administrator for Pesticides and Toxic Substances.

DCOs maintain a system to ensure that any TSCA CBI transmitted to other offices is received.

DCOs also maintain a current list of persons authorized access to TSCA CBI in their areas of responsibility and furnish this list, with any changes clearly indicated, to the Chief, ICB, on the first working day of each month.

DCOs keep on file a list furnished by the Chief, ICB, of DCOs and DCAs throughout EPA and, in a secure manner, a record of the locations and combinations of all locks, safes, and cabinets that protect TSCA CBI within their areas of responsibility. (DCOs ensure that these combinations are changed as required by Chapter III.B.)

DCOs are required to conduct periodic audits, at least annually, of all TSCA CBI in their areas of responsibility.

Before releasing TSCA CBI to any EPA employee, the DCO must verify that he/she is on the Authorized Access List.

The DCO must verify the identity of any submitter representative sent to EPA by a company to review or retrieve that company's previously submitted TSCA CBI before allowing access.

When an employee on the TSCA CBI Authorized Access List terminates or transfers, the DCO obtains a Confidentiality Agreement for United States Employees upon Termination or Transfer and keeps it on file for 5 years.

When releasing information that will be held overnight or longer, the DCO must ensure that an approved storage facility will be used prior to the release of such information.

DCOs also:

- Authorize and supervise the reproduction and destruction of TSCA CBI.
- Provide document control and handling services to those EPA components without a DCO.
- Direct DCAs in their areas of responsibility.

J. Document Control Officers (and Document Control Assistants) Approved for Computer Access

In addition to the responsibilities listed above, DCOs and DCAs approved for computer access are responsible for preparing input to, and receiving output from, authorized computer facilities. Specifically, their responsibilities include: keeping their computer access keys and passwords confidential, changing their keys and passwords frequently, ensuring that TSCA CBI is transmitted to authorized computer facilities only, and ensuring that use of the computer facility is in accordance with any restrictions placed on that use by the DAA/OTS or his/her designee.

K. Computer DCOs

In addition to the responsibilities listed in Chapter II.H. and II.I, computer DCOs are responsible for the control and security of all TSCA CBI contained within the computer facility. Specifically, they must maintain a system to ensure that physical and electronic access to TSCA CBI contained in the facility is restricted to authorized computer support personnel inside the

facility, and to authorized DCOs and DCAs outside the facility. They must ensure that the TSCA security requirements specified in Chapter IV are satisfied by the computer facility and must notify the DAA/OTS or his/her designee and the OIG of any alleged violations or incidents possibly involving unauthorized disclosure, modification, or destruction of user data or programs associated with TSCA CBI. When there is evidence of procedural violations but not of unauthorized disclosure, only the DAA/OTS must be notified.

L. Document Control Assistants (DCAs)

DCAs are responsible for performing any duties assigned to them by the DCO to whom they report. In the absence of the DCO, the DCA may act for him/her in routine matters. Difficult, unusual, or nonroutine questions or situations shall be referred to a DCO.

M. EPA Employees

Employees are responsible for the control and security of all TSCA CBI received by them. Specifically, they are required to discuss TSCA CBI only with authorized persons and safeguard TSCA CBI when in actual use as specified in Chapter III.C. Employees shall not discuss TSCA CBI over the telephone except as authorized by Chapter III.C.3. When working with submitter representatives, EPA employees must verify their identity before discussing with them any of their company's previously submitted TSCA CBI.

Employees who have TSCA CBI in their possession must store it in approved storage containers when it is not in use and at the close of each business day.

They must also safeguard the combinations to locks, safes, and rooms in which TSCA CBI is stored. EPA employees cannot make copies of TSCA CBI documents. If they need copies reproduced, they must obtain them through the DCO/DCA.

Employees with computer access authorization are responsible for keeping their computer access keys and passwords confidential and changing them frequently, and for using the computer facility in accordance with any restrictions placed on that use by the DAA/OTS.

Most importantly, employees must report immediately any alleged violations of TSCA or any violation of these procedures to their Division Director or equivalent.

N. Security Representatives

Security Representatives are responsible for assisting their Regions and Laboratories in establishing and maintaining the safeguards as prescribed by this Manual and assisting the EPA Headquarters Security Branch, ICB, and the OIG with security matters in their facilities.

III. Procedures for Handling TSCA Confidential Business Information

A. Gaining Access

To obtain a document containing TSCA CBI, the authorized person will request the document from the appropriate DCO/DCA who will verify that the requester is on the TSCA CBI Authorized Access List.

The DCO/DCA will then obtain the document from either local secure storage, another DCO, or an authorized computer facility.

If the requester has access to an acceptable storage cabinet, he/she may check the document out for a maximum of 90 days, renewable at the discretion of the DCO/DCA; otherwise, the document must be returned to the DCO/DCA by close of business the same day it is logged out.

The DCO/DCA will enter the appropriate information in the User Sign Out Log and will ensure that the document has a document control number, a cover sheet, and, at a minimum, a CBI stamp on the first page and the back of the last page, before releasing the document, whenever these things have not already been done.

B. Storage

1. *At EPA*

TSCA CBI must be stored as specified in this section. When it is not in use and at the close of business each day, TSCA CBI must be stored, at a minimum, within a metal cabinet with a bar and an EPA-approved three-way changeable combination padlock.

When warranted by the volume of CBI, the DAA/OTS may authorize secure document storage rooms and/or secure areas, provided they are approved, prior to use, by ICB and access is strictly controlled. Document storage rooms may incorporate one or more of the following, depending upon the location, construction, and configuration of the room:

- Combination-lock doors.
- Electronic Card Entry Systems.
- Contact alarm doors/windows.
- Ultrasonic alarms.
- Vibration alarms.
- Other remote intrusion alarms.

With the approval of the ICB, open storage is acceptable in such secure rooms or areas.

Combinations to cabinets and/or rooms where TSCA CBI is stored may only be issued to authorized persons who have a need to know. Combinations must be changed once a year or every time a person who knows a combination terminates or transfers, whichever comes first. The appropriate DCO must be notified of any changed combinations.

2. *When Traveling*

With the approval of a Division Director, TSCA CBI may be taken home by EPA employees prior to a trip when it would be impractical to return to the office to pick up the information. Employees will take all reasonable measures to safeguard the information. When traveling by plane or other public conveyance, employees must keep TSCA CBI in their possession and may not check it with their luggage.

When an employee is traveling with TSCA CBI (including samples) and is unable to deliver or ship the CBI to an authorized facility, TSCA CBI may be stored (for as short a period as possible) inside a locked container inside a locking portion of a motor vehicle. TSCA CBI may be stored in hotel safes.

C. Safeguards During Use

Confidential business information, when in use by an authorized person, must be protected at all times. TSCA CBI must be kept under the constant surveillance of an authorized person who is in a physical position to exercise direct security control over the material. It must be covered, turned face down, placed in approved storage containers, or otherwise protected when unauthorized persons are present. When not in use and at the close of each business day, TSCA CBI must be returned to approved storage containers.

Employees may discuss TSCA CBI only with other authorized persons. To transfer custody of a TSCA CBI document to another authorized person, an employee must go through the local DCO/DCA or, within a DCO's area of responsibility, use a Loan Receipt for TSCA CBI (Appendix XI). The Loan Receipt must be given to the DCO/DCA and the loaner should retain a copy. The recipient must also sign the cover sheet if he/she has not signed it previously.

1. *Secretarial Procedures*

Only persons listed on the TSCA CBI Authorized Access List may type documents that contain TSCA CBI. At all times the typist must safeguard the original, all "mag" cards, disks or other recording media, one-time carbon ribbons, drafts, scratch paper, notes, and any other materials containing TSCA CBI. The typist may not make carbons or copies of TSCA CBI documents.

When typing documents containing TSCA CBI, the typist must take all reasonable measures to ensure that no unauthorized person can see or otherwise gain access to what is being typed.

If the keyboard and printer are separate units, both must be under the direct physical control of the using employee. If a processing unit or storage medium is part of the system, and if either can be electronically or physically accessed by other persons, then the entire system must be approved by the ICB prior to use. MIDSD may be asked for assistance in evaluating the security of the system.

Whenever it is necessary to stop before a task is finished (at lunchtime or at the end of the day, for example), the typist must take all materials that contain TSCA CBI to the author for safeguarding or lock them up in an approved storage container. The typist shall check to be sure he/she has left nothing on the desk or in the typewriter or word-processor, etc., that might permit the unauthorized disclosure of TSCA CBI.

When the typing task is completed, the typist must take the original and all other materials to the author, who will in turn take them to the DCO/DCA. The DCO/DCA will enter the original into the document control system and destroy all other materials.

2. *Incoming Mail from Businesses*

Businesses should transmit TSCA CBI to EPA by registered mail, return receipt requested, in a double envelope. The inner envelope should be addressed specifically to the appropriate DCO/DCA with the following additional wording on the front: "TSCA Confidential Business Information--To Be Opened By Addressee Only." The outer envelope should be addressed to the apropriate DCO/DCA without the additional wording. Any incoming mail so addressed must be taken to the appropriate DCO/DCA immediately. Also, any TSCA correspondence that is marked "confidential," "proprietary information," "company secret," etc., or otherwise contains a request for confidential treatment, must be taken to the DCO/DCA immediately.

Employees are responsible for safeguarding any unlogged TSCA CBI in their possession. Also, whenever an employee becomes aware that correspondence contains TSCA CBI, whether it has been properly designated or not, the employee must take it to the appropriate DCO/DCA immediately. If the DCO/DCA is not available, the CBI must be secured until he/she is available.

3. *Telephone Calls*

With the written approval of a Division Director, authorized EPA employees may discuss TSCA CBI over the telephone with other authorized EPA employees in Headquarters and other EPA offices and with authorized EPA contractors.

With the written approval of a Division Director, EPA employees may discuss TSCA CBI on the telephone with authorized Federal employees in other agencies or their authorized contractors. The EPA employee must verify that the other person is authorized for access and must also indicate at what point in the conversation TSCA CBI is to be discussed.

If the EPA employee is not sure that the other person is authorized access to TSCA CBI, he or she will check the EPA TSCA CBI Access List, which is maintained by each DCO.

With the permission of the submitter and after verifying his/her identity, authorized EPA employees may discuss TSCA CBI over the telephone with the submitter. If submitters discuss CBI over the telephone, employees shall notify them that such discussion does not constitute a waiver of any CBI claim.

Between EPA and a submitter, with the permission of the submitter, TSCA CBI may be transmitted electronically through communications lines (e.g., by telecopier). See Section IV.B.8. before electronically transmitting any TSCA CBI. When an EPA employee requests additional information over the telephone from a submitter, the employee should also inform the submitter that the additional information may be claimed to be CBI.

4. *Meetings*

For any meeting, symposium, panel discussion, or seminar at which TSCA CBI will be discussed, the meeting chairperson shall provide a TSCA CBI Sign-In Sheet (Appendix XI) if there are attendees who have not had prior access to the TSCA CBI to be discussed. In addition, the chairperson will retain the option to require a sign-in sheet whenever he/she thinks it necessary. All attendees must sign it and record their EPA identification badge number. The chairperson shall give the sign-in sheet to the local DCO/DCA who will retain it for 1 year.

The chairperson must also ensure that only authorized persons are present and shall announce that TSCA CBI is to be discussed. When necessary, the chairperson shall review with the attendees their responsibility for safeguarding CBI in any and all forms, including, but not limited to, any notes taken and any subsequent discussions.

No recording is to be made of the meeting unless the chairperson has authorized it. If authorized, the recording must be treated as all other confidential business information and entered into the document control system.

The meeting room shall be secured after the meeting by the chairperson. This includes cleaning all chalkboards, destroying, by approved methods, all tear sheets and other notes, and ensuring that nothing is left in the room that could lead to the unauthorized disclosure of TSCA CBI.

When notes containing TSCA CBI are taken from a document, a meeting, or any other source, the notes must be protected as TSCA CBI. If the notes are to be circulated to other authorized persons, they must be entered into the document control system. The taking of notes is discouraged and should be kept to a practical minimum. Any document generated from notes shall be treated as described in section H of this chapter.

5. *Lost or Unaccounted-for Documents*

If any employee becomes aware that a TSCA Confidential Business Information document is lost or otherwise unaccounted for, he/she shall immediately notify the appropriate local DCO/DCA. If the DCO/DCA verifies that the document is lost or otherwise unaccounted for, he/she shall notify his/her Division

Director. If, after a thorough search, but not later than 3 working days after such discovery, the document is not found or accounted for, the Office of the Inspector General will be notified in writing and will initiate an investigation. The Chief, ICB, will also be notified.

D. Transmittal

1. *Within an EPA Facility*

Within an EPA facility, TSCA Confidential Business Information shall be hand-delivered only, by one authorized person to another. At no time shall TSCA CBI be transmitted through interoffice mailing channels.

2. *Outside an EPA Facility*

Ordinarily, TSCA CBI will be transmitted by registered mail, return receipt requested, in a double envelope. On the inner envelope must be the name and address of the recipient with the following additional wording on the front: "TSCA Confidential Business Information--To Be Opened By Addressee Only." The outer envelope will have only the recipient's name and address, without the additional wording.

When registered mail would take too long or other circumstances warrant it, the Express Mail Service of the U.S. Postal Service, or private carriers approved by ICB may be used for transmitting TSCA CBI. Written approval by a Division Director or equivalent is required for such transmittals. A return receipt of some type must be included inside the inner package or envelope.

Physical samples, such as those collected during a TSCA inspection, which are claimed to be TSCA CBI, shall be placed in a package or container and the seal marked "TSCA Confidential Business Information." Such samples shall be delivered or shipped as soon as possible to the appropriate DCO/DCA in the Laboratory. If shipping or delivering is not immediately possible, as when an employee is traveling, the sample shall be stored inside a locked container inside a locking portion of a motor vehicle or in a hotel safe.

Authorized persons may hand-carry TSCA CBI to other EPA facilities or to persons outside EPA, providing the dispatching DCO maintains a record and obtains a receipt from the person at the facility receiving the information. Information being hand-carried shall be packaged as registered mail or in an alternate manner approved by ICB.

When circumstances warrant, and with ICB approval, special arrangements may be made for transporting of CBI within a local area, e.g., the Washington, D.C., metropolitan area.

E. Reproduction/Destruction

1. *Reproduction*

TSCA CBI may not be reproduced except upon approval by and under the supervision of a DCO/DCA. Reproduction shall be kept to an absolute minimum. Whenever possible, reproduction shall be done by or in the presence of a DCO/DCA. The DCO/DCA shall enter all copies into the document control system and apply the same control requirements to the copies as those for the original.

2. *Destruction*

TSCA CBI documents may not be destroyed except upon approval by and under the supervision of a DCO/DCA. Destruction must be by shredding, burning, or other means approved by ICB. The DCO/DCA shall remove the cover sheet, make a notation of the destruction on the cover sheet, and return it to originating DCO/DCA. That DCO/DCA shall keep a record of the destruction in the Destruction Log (Appendix IV).

F. Photographs

Whenever it is necessary to take photographs that contain TSCA CBI, as during a TSCA inspection, either an "instant" camera must be used or the film must be processed by an authorized EPA photo lab or an authorized private photo lab contractor. The Chief, ICB, will maintain a list of facilities cleared to process film containing TSCA CBI.

G. Retiring of Documents

When TSCA CBI documents are to be retired for legal, historical, or reference purposes, they shall be shipped to the Federal Records Center in accordance with the procedures in the EPA *Records Management Manual*. Appropriate steps will be taken to ensure that TSCA CBI is properly protected for as long as necessary.

H. Generating TSCA Confidential Business Information Documents

When an EPA employee generates a document from an existing TSCA CBI document(s) the generated document shall be presumed to contain TSCA CBI and be protected accordingly. If there is a question as to whether a staff-generated document in its final form contains TSCA CBI, it will be taken to the Branch Chief, who will determine whether or not the document contains TSCA CBI. If the Branch Chief determines that the document contains TSCA CBI, it will be taken to the DCO immediately, who will enter it into the document control system. Generation of such documents shall be kept to a minimum.

I. Retaining Logs

All logs maintained under these procedures shall be retained for at least 5 years.

IV. Security Requirements for EPA Computer Centers

A. General

In addition to the applicable Federal statutes and regulations cited in Chapter I.C. of this Manual, the computer processing of TSCA CBI must be in compliance with the following directives issued to all Federal agencies processing sensitive data by computer:

- Office of Management and Budget OMB Circular A-71
- Office of Personnel Management FPM Ltr. 732-7
- National Bureau of Standards FIPS PUBS
- General Services Administration 41 CFR, Ch. 101

All TSCA computer support facilities, whether dedicated to CBI processing or shared with non-CBI programs, must meet the basic requirements for protection of TSCA CBI.

1. *Basic Security Requirement*

The system must provide a level of security adequate to protect TSCA CBI being processed from unauthorized access by users and other persons having access to the facility.

2. *Computer Center Security Plan*

The Computer DCO shall develop, maintain, and perform periodic audits against a plan containing a comprehensive set of documented data security standards and procedures. This plan must provide for periodic risk analyses and for obtaining confidentiality agreements from all contractor and subcontractor personnel working for the facility (such as equipment maintenance contractors) and must meet all requirements specified below. This security plan is subject to approval by the DAA/OTS or his/her designee and shall be available to representatives of EPA's OIG.

B. Hardware and Software Characteristics

1. *Hardware*

The computer hardware supporting the system must be capable of maintaining isolation between user tasks, and must prevent normal users from executing instructions reserved for the operating system.

Since a well-designed system of software, as specified below, can adequately compensate for many desirable hardware features, no further specific hardware requirements are set forth here.

2. *Software System Design*

The operating system must have data security as one of its primary design requirements. The operating system must provide mechanisms to implement the following principles.

Note that software system design requirements a. and b., below, are essentially identical to the hardware requirements specified above and may substitute for the hardware requirement, if proven effective.

a. *User/Task Isolation*

Separate users or tasks operating concurrently in the system must be, within system limits, totally isolated from one another.

b. *Control of Interfaces and Security-Sensitive Work Spaces*

Operating system interfaces must prevent users from gaining access to instructions or data reserved for the operating system. The operating system shall not use user-accessible work areas for passwords or other security-sensitive data.

c. *Audit Trails*

The system must provide extensive auditing data to record significant system activities that are of a security concern, such as log-on attempts, file accesses, and program execution. The system shall also provide to EPA a list of attempts at unauthorized access of EPA data files and/or programs by users and others.

d. *User Identification and Authorization*

Mechanisms in the operating system must be capable of identifying individual users of the system and specifying the system resources and privileges to which the user is authorized.

3. *Applications Software Management*

Any employee responsible for developing software that will process TSCA CBI is required to prepare an ADP Application Security Plan. This plan describes the components of the system or subsystems that may be accessible by authorized DCOs and DCAs including computer programs, inputs, outputs, and data bases. The security plan must also state how security is to be enforced, and, in particular, how unauthorized modifications to the programs will be prevented.

The plan must also address controls to ensure data integrity and systems assurance, including audit trails. The plan must be reviewed and approved by the DAA/OTS or his/her designee following review by the Director of the Management Information and Data Systems Division, and the OIG. The program instituted must be periodically reviewed for effectiveness and shall be subject to periodic audit.

4. *File-Catalog Structure*

The operating system must provide resource control at the file level that permits isolation of one user's files from another's. It shall not be possible for one user to access another's files simply by having knowledge of the file name and account number.

5. *File Access Control/Permission Mechanism*

The operating system shall provide for file access through a specific permission mechanism capable of the following.

a. *Specific User Permissions*

It shall be possible to give selected users access to a particular file without giving all users access to the file.

b. *Access Type Control*

It shall be possible for a file owner to restrict the type of access to a file. Two minimum categories must be supported--Read Only Access and Read/Write Access. It is also highly desirable to be able to restrict access to program files on an execute-only (i.e., no read) basis and to restrict "control" access to files (i.e., scratching or renaming the file).

6. *User Features*

To enable user flexibility in adding security features to applications, the system shall provide a range of optional protection features, including the following.

a. *Password Change Capability*

Individual users (DCOs and DCAs authorized for computer access) shall ensure that their own log-on and file access passwords are changed at frequent intervals.

b. *Idle Terminal Disconnect*

The system shall provide a mechanism to automatically disconnect a user terminal after a fixed period of no activity. If the terminal is a CRT type, then the system shall clear the screen before the automatic disconnect.

7. *Communications Facilities*

The communications network must be adequately protected against intentional or accidental misrouting of data traffic. Line protocol and concentrator-modem interfaces shall be designed to detect and protect against anomalous events (such as spurious data or line disconnects) that might otherwise cause misrouting or loss of data.

Communications equipment (modems, multiplexors, concentrators, etc.) shall be located in secure areas accessible only to authorized personnel.

8. *Electronic Transmission of TSCA CBI*

When TSCA CBI is transmitted electronically through communications lines, such lines must be protected in accordance with the National Bureau of Standards' Data Encryption Standards. Such encryption is not required for hardwired connections within a secure facility.

Any terminal or printer used to read or print TSCA CBI must be located in a secure room and used for this purpose only by a person with computer-access authorization.

C. Media Handling

Policies and procedures must be included in the security plans (Chapter IV.A.2. and IV.B.3.) to fully control access to and handling of various data media used in processing TSCA CBI, including magnetic tape, disk packs, printed output, cards, micrographic output, and other such media.

1. *Media Labeling*

Media must be labeled only with such information as is necessary for retrieval and media management.

2. *Separation of Storage Facilities*

Storage areas for various media, including mountable volumes, must be separate from the machine operations areas.

3. *Transmittal of Media*

Input and output media can be transmitted only between the Computer DCO and the appropriate program area DCO. In no case shall input media be accepted from or delivered to a third party. Positive user identification procedures must be in effect. Detailed logs of all media transmitted to and from the computer facility must be maintained.

4. *Disposal of Media*

When authorized in writing by a DCO, media will be disposed of by the Computer DCO in a manner that will prevent any disclosure of data to outside parties.

D. Facility Protection

All necessary steps are to be taken to protect facilities, equipment, and the data they contain from inadvertent or intentional access, damage, or destruction.

1. *Access Control*

The computer DCO is required to enforce a policy of permitting no unescorted visitors into computer operations areas or into areas where sensitive data are handled. Only designated personnel with an ongoing need to know will be authorized unescorted access to such areas.

2. *Facility Security System*

Any computer facility processing TSCA CBI must have, prior to receiving such data, an adequate facility or building security system to protect both the equipment and data that has been approved by the ICB.

E. Backup and Recovery Capability

There shall be documented procedures to ensure adequate backup and recovery capability in the event of loss of data or processing capability through accident or disaster. These procedures shall include a provision for periodic testing of the backup and recovery capabilities.

1. *File Backup*

All files resident on the system shall be copied onto backup media on a regular basis.

2. *Off-Site Storage*

A complement of backup files that will enable recovery to the previous end-of-week position in the event of a major disaster resulting in loss of on-site copies shall be stored off-site. An off-site storage facility is defined as one that is so located that it is highly unlikely to be affected by a major disaster (fire, explosion, etc.) striking the main facility. Off-site storage must be as secure as that at the primary location of data and must be approved by ICB.

V. Security Requirements for Other Federal Agencies

A. Purpose

This section sets forth the circumstances and procedures under which TSCA CBI may be furnished by EPA to another Federal agency that has responsibility under law for the protection of health or the environment or for specific law enforcement purposes.

B. Policy

EPA policy is to furnish TSCA CBI to any Federal agency with responsibility under any law for the protection of health or the environment or for specific law enforcement purposes, provided the other agency is able and willing to meet prescribed standards for ensuring the security of the information and promises to treat the information as confidential in accordance with 40 CFR Part 2.

C. Procedures for Answering Requests

Any EPA office that receives a written request from another Federal agency for access to TSCA CBI in accordance with 40 CFR Part 2 (other than requests made under section D. below), must refer the request to the Assistant Administrator for Pesticides and Toxic Substances (AA/OPTS).

The AA/OPTS or his/her designee must first evaluate the official need stated by the other Federal agency. If the need relates to the other agency's duties under a law for the protection of health or the environment or is for specific law enforcement purposes, the AA/OPTS must ensure that the other agency has agreed to keep the information confidential in accordance with the requirements of 40 CFR Part 2.

If the other Federal agency has met the requirements of 40 CFR Part 2, the AA/OPTS shall ask the agency to furnish copies of security procedures under which the agency proposes to protect the information. The procedures must provide at least the same degree of security provided by this Manual and include the requirement for obtaining signed copies of the TSCA Federal Non-EPA Employee Confidentiality Agreement (Appendix VII) from each of its employees who will have access, and obtaining signed copies of the Confidentiality Agreement for United States Employees Upon Termination or Transfer (Appendix VIII) from each employee who terminates or transfers. (This requirement does not apply to Department of Justice employees described in section E. below.)

If the other Federal agency has met the requirements of 40 CFR Part 2, there are two ways to meet EPA's requirement that its facilities and written procedures provide at least the same degree of protection for TSCA CBI as EPA provides. 1) The other Federal agency may develop its own procedures and forward them to EPA. The EPA OIG will determine if the procedures meet EPA's

minimum requirements and forward a report to the AA/OPTS. The AA/OPTS, with the assistance of ICB, will then determine whether the security procedures would provide at least the same degree of protection as procedures in this Manual. If so, the OIG will make a physical inspection of the other Federal agency's facilities to determine if they meet the requirements of the other Federal agency's approved procedures and report the results to the AA/OPTS. 2) The other Federal agency may adopt EPA's security procedures. If they do, the OIG will inspect their facilities and report to the AA/OPTS as in number 1.

In both cases, upon the approval of the AA/OPTS, TSCA CBI may be furnished to the other agency in accordance with established procedures, including the use of the Federal agency sign out log.

If the other agency is authorized to receive TSCA CBI and if the applicable procedures in 40 CFR Part 2 have been followed, the AA/OPTS shall notify the appropriate DCO who shall provide the information in accordance with established procedures.

D. Procedures for Interagency Agreements

If a particular Federal agency has a continuing need for TSCA CBI, the AA/OPTS may negotiate an interagency agreement (IAG) with that agency to provide access to TSCA CBI, in accordance with EPA order 1610. The IAG must meet all the requirements of section C. above and specify the procedures that will be followed by the other agency in making specific requests for information under the IAG and to whom the requests will be addressed.

The AA/OPTS, or his/her designee, shall notify the appropriate DCOs of the agreement and the procedures to be followed in responding to specific requests.

Under such an agreement, if the applicable procedures in 40 CFR Part 2 have been followed, a DCO may furnish confidential business information to another Federal agency, in accordance with established procedures, without receiving specific authorization from the AA/OPTS for each request.

E. Exemption for the Department of Justice

Department of Justice (DOJ) employees may be furnished TSCA CBI when prosecuting cases under TSCA or providing legal assistance to EPA. The Department of Justice, including the FBI, shall be presumed to meet EPA's security requirements. No security plans need be submitted and no inspection of facilities is required. DOJ employees are not required to sign a confidentiality agreement. However, the receiving DOJ office will be apprised of the need to maintain appropriate security controls on all TSCA CBI furnished them.

Any transfer of TSCA CBI documents from EPA to DOJ must be accomplished through an EPA DCO/DCA, and all requirements for security of CBI during transmission must be met.

Authorized EPA employees, when necessary and with permission of a Division Director or above, may discuss TSCA CBI with appropriate DOJ employees, either in person or on the phone. Any TSCA CBI discussed will be clearly identified as such.

F. Limited Access

Individual employees of other Federal agencies may be permitted to review TSCA CBI onsite at EPA with the permission of the appropriate EPA Division Director or equivalent. The Authorization for Access form should be used, along with the Confidentiality Agreement for non-EPA Federal Employees. Such individuals must be fully informed of their security responsibilities, must sign the cover sheet of any document to which they have access, and will be under direct EPA supervision at all times. No TSCA CBI will leave the EPA facility, and the individuals will be told that they may not discuss the information except with other employees of their agency granted access and authorized EPA employees, may not generate any notes or correspondence containing CBI, and may not discuss the CBI on the telephone.

G. Violations

Any violation of another Federal agency's security procedures, even when there is no evidence of wrongful disclosure, shall be investigated by that agency and appropriate remedial action taken. Results of the investigation and subsequent action must be forwarded to EPA's OIG and ICB.

Any alleged or actual wrongful disclosure of TSCA CBI by an employee of another Federal agency shall be reported immediately by that agency to the EPA OIG and the Assistant Administrator for Pesticides and Toxic Substances.

Violations of the security provisions of an interagency agreement under this chapter shall be investigated when appropriate by the OIG, which shall report to the AA/OPTS. If the AA/OPTS finds that the other agency has violated the terms of the interagency agreement, he/she may terminate that agency's right of access pending resolution of the matter.

If the investigation by the OIG develops information indicating a criminal violation, the case shall be referred to the Department of Justice. When the Department of Justice accepts jurisdiction, any further action, including notification of the business involved, will be dictated by them.

Appendix I

EXCERPTS FROM *EPA Conduct and Discipline Manual*

GENERAL

The achievement of constructive discipline [here, of course, we mean discipline as it relates to compliance with the requirements of the *TSCA CBI Security Manual* is a responsibility of supervisors. An atmosphere of constructive discipline is brought about by a supervisor's good example and practice, instruction, fair and equal treatment of all employees, and firm and decisive leadership.

DETERMINING CORRECTIVE ACTION TO BE TAKEN

Supervisors and management officials at all levels are responsible for maintaining discipline in their organizations by taking appropriate corrective actions. . . . Any supervisor or management official with supervisory duties may take informal corrective actions and issue official reprimands unless this authority has been specifically withheld. The following principles will be observed in the exercise of both formal and informal correction action:

The action taken must be consistent with the precept of like penalties for like offenses with mitigating or aggravating circumstances taken into consideration. The action taken should be fair and equitable; and if a penalty is warranted, it should be no more severe than sound judgment indicates is required to correct the situation and maintain discipline.

When the appropriate corrective action is being determined, it should be established whether the employee knew, or could reasonably be expected to know, what standard of conduct or performance was expected of him.

Repetition of the same offense must be considered in the assessing of any penalty, as such repetition implies a disregard for authority.

INFORMAL CORRECTIVE ACTIONS

When a supervisor decides that corrective action is necessary, he should first consider informal measures which are nonpunitive in nature but which will instruct offending employees and remedy problem situations. Supervisors are urged to review the background of individual cases and assure that informal measures are considered before formal corrective actions, which are recorded in an employee's official personnel folder, are utilized:

- Closer Supervision

- On-the-Job Training

- Oral Reprimands--Perhaps the most common of corrective actions is the face-to-face session between employee and supervisor. To be most effective, such discussions should be conducted in private without undue embarrassment to the employee. . . . Basic facts of the discussion, including the reason for the reprimand and the corrective steps necessary, should be recorded in a memorandum for file and maintained in local files. No record of such informal discussions may be placed in an employee's personnel folder.

- Written Warnings--This kind of corrective measure lacks the give and take of the oral interview and should usually be employed only if the supervisor has already tried an oral warning or feels that it would be inappropriate. A written warning should describe exactly what improper actions the employee is engaging in, and outline positive corrective steps, and state what penalty might result if the actions continue. A copy of the written warning should not be placed in the employee's official personnel folder, but copies should be retained in the supervisor's local files. Written warnings are often effective in influencing those employees who require a more tangible expression of a supervisor's views.

FORMAL DISCIPLINARY ACTIONS

A formal disciplinary action may be an official written reprimand, a suspension, a change to a lower grade, or removal. Records of formal disciplinary actions become a part of the employee's official personnel folder. Supervisors should initiate such actions only after coordinating any proposed action with their operating personnel officers. [Detailed information concerning these actions is contained in Chapter 5 of the *Conduct and Discipline Manual*.]

REASSIGNMENT AS A CORRECTIVE ACTION

Reassignment of personnel may serve as a useful corrective tool and is a valid disciplinary action. If an employee is considered to have the skills and desires needed to successfully perform at his grade level but is unable to function effectively in his immediate work situation, a reassignment to a new environment may be considered. In other cases, a reassignment to a position where closer supervision is possible [or access to TSCA CBI is not required] can prove beneficial to both the employee and EPA.

EXCERPTS FROM APPENDIX C, TABLE OF OFFENSES AND PENALTIES

When [formal] disciplinary action becomes necessary, this guide should be used in order to facilitate comparable action throughout the Agency in comparable cases. Penalties for offenses usually will fall within

the ranges indicated, but in unusual circumstances greater or lesser penalties may be applied unless otherwise provided by law.

When disciplinary action is being determined in a specific case, consideration should be given to the record of the employee, and, when there is a repetition of offenses, to the time interval between offenses.

When an employee has committed a combination or series of different offenses, a greater penalty than is listed for a single offense should be considered.

NATURE OF OFFENSE	FIRST OFFENSE	SECOND OFFENSE	THIRD OFFENSE
Violation of security regulations involving other than classified [national defense] information	Oral/written reprimand	Written reprimand to 1-day suspension	5-day suspension to removal
Failure to assess a penalty when the facts are known and warrant disciplinary action	Written reprimand to 5-day suspension	10-day suspension to 30-day suspension	Removal

Appendix II

(Actual Size 8 1/2" x 11")

TSCA CBI
WHEN FILLED IN

U.S. ENVIRONMENTAL PROTECTION AGENCY
INVENTORY LOG
TSCA CONFIDENTIAL BUSINESS INFORMATION

DOES NOT CONTAIN NATIONAL SECURITY INFORMATION (E.O. 12065)

DATE RECEIVED	DOCUMENT CONTROL NO.	NO. PAGES	RECEIVED FROM *(Enter company, city, and state)*	DESCRIPTION	DISPOSITION

Appendix III

(Actual Size 8 1/2" x 11")

TSCA CBI WHEN FILLED IN		U.S. ENVIRONMENTAL PROTECTION AGENCY USER SIGN OUT LOG TSCA CONFIDENTIAL BUSINESS INFORMATION		DOES NOT CONTAIN NATIONAL SECURITY INFORMATION (E.O. 10865)		
DATE CHECKED OUT	DOCUMENT CONTROL NO./ COPY NO.	USER INFORMATION		DATE RETURNED	DCO INITIAL	DISPOSITION
		EPA ID NO.	SIGNATURE			

EPA Form 7710-11 (Rev. 9-81) Previous edition is obsolete.

Appendix IV

(Actual Size 8 1/2" x 11")

TSCA CBI
WHEN FILLED IN

U.S. ENVIRONMENTAL PROTECTION AGENCY
DESTRUCTION LOG
TSCA CONFIDENTIAL BUSINESS INFORMATION

DOES NOT CONTAIN
NATIONAL SECURITY
INFORMATION
(E.O. 12065)

DC)/DCA NAME _____ LOCATION _____

DATE DE-STROYED	DOCUMENT CONTROL NUMBER	DESCRIPTION	DCO/DCA SIGNATURE

EPA Form 7710-45 (9-81)

Appendix V

(Actual Size 8 1/2" x 11")

TSCA CBI
WHEN FILLED IN

U.S. ENVIRONMENTAL PROTECTION AGENCY
CONTRACTOR/SUBCONTRACTOR SIGN OUT LOG
TSCA CONFIDENTIAL BUSINESS INFORMATION

DOES NOT CONTAIN NATIONAL SECURITY INFORMATION (E.O. 12065)

DATE OUT	EPA DOCUMENT CONTROL NO./COPY NO.	NO. PAGES	DESCRIPTION	(SUB)CONTRACTOR/ (SUB)CONTRACT NO.	EPA PROJECT OFFICER	DCO INITIAL	RECEIPT	DATE RETURNED	DCO INITIAL

EPA Form 7710-12 (Rev. 9-81) Previous edition is obsolete.

Appendix VI

(Actual Size 8 1/2" x 11")

TSCA CBI WHEN FILLED IN	U.S. ENVIRONMENTAL PROTECTION AGENCY FEDERAL AGENCY, CONGRESS, AND FEDERAL COURT SIGN OUT LOG TSCA CONFIDENTIAL BUSINESS INFORMATION					DOES NOT CONTAIN NATIONAL SECURITY INFORMATION (E.O. 12065)			
DATE OUT	EPA DOCUMENT CONTROL NO./COPY NO.	NO. PAGES	DESCRIPTION	FEDERAL AGENCY, CONGRESS, COURT	RECIPIENT	DCO INITIAL	RECEIPT	DATE RETURNED	DCO INITIAL

EPA Form 7710-13 (Rev. 9-81) Previous edition is obsolete.

Appendix VII

(Front)

(Actual Size 8 1/2" x 11")

REQUEST FOR APPROVAL OF CONTRACTOR ACCESS TO TSCA CONFIDENTIAL BUSINESS INFORMATION

Requesting Official*	Signature	Date
Title and Office		
Contractor and contract number (if modification)		
I. Brief description of contract, including purpose, scope, length, and other important details. (Continue on the back of this form if necessary.)		
II. What TSCA CBI will be required, and why? (Continue on back if necessary.)		
III. Will computer access to TSCA CBI be required by the contract? If so, explain why and to what extent on the back of this form.		
If you approve this request, this office will initiate procedures to ensure compliance with the "TSCA CBI Security Manual" and "Contractor Requirements for the Control and Security of TSCA Confidential Business Information."		

*Must be Division Director (or equivalent) or above.

Office Director for
Toxic Substances

Approved _____

Date _____

EPA Form 7710-15a (9-81)

Appendix VIII

CONFIDENTIALITY AGREEMENT

FOR UNITED STATES EMPLOYEES

UPON TERMINATION OR TRANSFER

In accordance with my official duties as an employee of the United States, I have had access to Confidential Business Information under the Toxic Substances Control Act (TSCA) (15 U.S.C. § 2601 et seq.). I understand that TSCA CBI may not be disclosed except as authorized by TSCA or Agency regulations.

I certify that I have returned all copies of any TSCA CBI in my possession to the appropriate document control officer specified in the procedures set forth in the *TSCA Confidential Business Information Security Manual*.

I agree that I will not remove any copies of TSCA CBI from the premises of the Agency upon my termination or transfer. I further agree that I will not disclose any TSCA CBI to any person after my termination or transfer.

I understand that as an employee of the United States who has had access to TSCA CBI, under section 14(d) of TSCA [15 U.S.C. § 2613 (d)] I am liable for a possible fine of up to $5,000 and/or imprisonment for up to 1 year if I willfully disclose TSCA CBI to any person.

If I am still employed by the United States, I also understand that I may be subject to disciplinary action for violation of this agreement.

I am aware that I may be subject to criminal penalties under 18 U.S.C. § 1001 if I have made any statement of material facts knowing that such statement is false or if I willfully conceal any material fact.

_____ _____

Signature Date

_____ _____

Name I.D. Number

Appendix IX

(Actual Size 8 1/2" x 11"
Printed on Heavy,
Dark Green Paper Stock)

TSCA CONFIDENTIAL BUSINESS INFORMATION

DOES NOT CONTAIN NATIONAL SECURITY INFORMATION *(E.O. 12065)*

DOCUMENT CONTROL OFFICER	DOCUMENT CONTROL NO.	DATE RECEIVED

The attached document contains Confidential Business Information obtained under the Toxic Substances Control Act *(TSCA, 15 U.S.C. 2601 et seq.)*. TSCA Confidential Business Information may not be disclosed further or copied by you except as authorized in the procedures set forth in the TSCA CONFIDENTIAL BUSINESS INFORMATION SECURITY MANUAL.

If you willfully disclose TSCA Confidential Business Information to any person not authorized to receive it, you may be liable under section 14*(d)* of TSCA *(15 U.S.C. 2613(d))* for a possible fine up to $5,000 and/or imprisonment for up to one year. In addition, disclosure of TSCA Confidential Business Information or violation of the procedures cited above may subject you to disciplinary action with penalties ranging up to and including dismissal.

Each person who is given access to this document must fill in the information below the first time that he/she has access.

LAST NAME	SIGNATURE	EPA ID NO.	DATE

DO NOT DETACH

EPA Form 7710-6 (Rev. 5-80) PREVIOUS EDITION MAY BE USED.

Appendix X

(Actual Size 8 1/2" x 11")

I. AUTHORIZATION FOR ACCESS TO TSCA CONFIDENTIAL BUSINESS INFORMATION (CBI)

Full Name	EPA ID Number	Position	Office (Incl. Division)

It is the responsibility of each Authorizing Official* to ensure that employees under his/her supervision who require access to TSCA CBI:

1. Complete the required investigative forms† prior to access to TSCA CBI
2. Sign the Confidentiality Agreement for EPA Employees
3. Are fully informed regarding their security responsibilities for TSCA CBI
4. Obtain access only to that TSCA CBI required to perform their official duties.

Signature of Authorizing Official _____ Date _____

Title _____ Location _____

II. APPOINTMENT OF DCOS/DCAS

If employee is being appointed DCO/DCA, authorizing official (Division Director at Headquarters, Regional Administrator or Laboratory Director in the field) must sign this section.

_____ Signature/Title

III. CONFIDENTIALITY AGREEMENT FOR EPA EMPLOYEES

I understand that I will have access to certain Confidential Business Information submitted under the Toxic Substance Control Act (TSCA, 15. U.S.C. 2601 *et seq.*). This access has been granted in accordance with my official duties as an employee of the Environmental Protection Agency.

I understand that TSCA CBI may not be disclosed except as authorized by TSCA and Agency regulations. I understand that under sections 14(d) of TSCA [15 U.S.C. 2613(d)] I am liable for a possible fine of up to $5,000 and/or imprisonment for up to one year if I willfully disclose TSCA CBI to any person not authorized to receive it. In addition, I understand that I may be subject to disciplinary action for violation of this agreement with penalties ranging up to and including dismissal.

I agree that I will treat any TSCA CBI furnished to me as confidential and that I will follow the procedures set forth in the *TSCA Confidential Business Information Security Manual.*

I have read and understand the procedures.

Signature _____ Date _____

IV. I certify that all necessary investigative forms‡ have been completed and forwarded to the Headquarters Security Branch.

Local DCO/DCA	Signature	Date	Phone

*Must be Division Director (or equivalent) or above.
†See revised Procedure for Becoming Authorized for Access to TSCA CBI.
‡For employees described in section I.G. under "exceptions" and those who require administrative full-field investigations.

EPA Form 7710-47 (9-81)

Appendix Xa

REQUEST FOR APPROVAL OF TEMPORARY EMPLOYEE FOR ACCESS TO TSCA CBI			DATE OF REQUEST
DIVISION DIRECTOR	PROGRAM OFFICE	TELEPHONE NUMBER	MAIL CODE
NAME OF EMPLOYEE		POSITION OCCUPIED	

The above named employee requires access to TSCA Confidential Business Information to perform his/her assigned duties. The individual falls into a category which requires approval of the Chief, Information Control Branch, prior to access being granted, and is also required to submit to the Security Branch the forms required to initiate a NACI Investigation: SF-171, Personal Qualifications Statement: SF-85, Date for Nonsensitive or Noncritical-Sensitive Position; and SF-87, United States Civil Service Commission Fingerprint Chart.

I authorize the above named employee to have access to TSCA CBI, contingent upon their submitting the appropriate forms to the Security Branch and subsequently submitting the usual TSCA Access Authorization Form through the normal channels.

SIGNATURE CHIEF, INFORMATION CONTROL BRANCH	DATE

I certify that the above named employee has submitted the necessary investigative forms to the Security Branch and has been fingerprinted.

SIGNATURE SECURITY BRANCH REPRESENTATIVE	DATE

RETURN TO

Return this completed form to the Program Office Division Director, with a copy to the Chief, Information Control Branch. Security Branch should also retain a copy.

EPA Form 7710-46 (9/81)

Appendix XI

LOAN RECEIPT FOR
TSCA CONFIDENTIAL BUSINESS INFORMATION

I acknowledge receipt of TSCA Confidential Business Information Document(s) listed below:

1a. DOCUMENT CONTROL NO.	1b. COPY NO.	6a. DOCUMENT CONTROL NO.	6b. COPY NO.
2a. DOCUMENT CONTROL NO.	2b. COPY NO.	7a. DOCUMENT CONTROL NO.	7b. COPY NO.
3a. DOCUMENT CONTROL NO.	3b. COPY NO.	8a. DOCUMENT CONTROL NO.	8b. COPY NO.
4a. DOCUMENT CONTROL NO.	4b. COPY NO.	9a. DOCUMENT CONTROL NO.	9b. COPY NO.
5a. DOCUMENT CONTROL NO.	5b. COPY NO.	10a. DOCUMENT CONTROL NO.	10b. COPY NO.

I understand that I am responsible for protecting these data in accordance with the *TSCA Confidential Business Information Security Manual*. Also that I am liable for a fine of up to $5,000 and/or imprisonment up to 1 year if I willfully disclose it to any unauthorized person. I may also be subject to disciplinary action up to and including dismissal for any violation of procedures for safeguarding these data.

NAME OF RECIPIENT	SIGNATURE OF RECIPIENT
NAME OF LOANER	DATE DOCUMENT(S) RECEIVED

EPA Form 7710-14 (Rev. 9/81)

Appendix XII

(Actual Size 8 1/2" x 11")

TSCA CONFIDENTIAL BUSINESS INFORMATION
MEETING SIGN-IN SHEET

DATE	TIME
MEETING PLACE *(Room, Building, City, State)*	CHAIRPERSON
SUBJECT OF MEETING	

NAME *(Print)*	SIGNATURE	OFFICE/DIVISION/BRANCH	EPA ID NO.

THIS SIGN-IN SHEET MUST BE GIVEN TO THE APPROPRIATE DCO/DCA

EPA Form 7710-44 (9/81)

Index

	Page
AA/OPTS, Responsibilities of	7
Access, Defined	4
Access, How To Gain	13
ADP Application Security Plan	
Defined	4
Discussed	22
Authorized Access List	3
Authorized Computer Facility, Defined	4
Authorized Person, Defined	4
Backup Capability	25
Chief, Information Control Branch, Responsibilities of	9
Chief, Security Branch, FSSD, Responsibilities of	9
Classification of EPA-Generated Documents	18
Combinations	14
Computer Center Security Plan	
Defined	4
Discussed	19
Computer Center Security Requirements	19
Computer DCO, Defined	4
Computer DCOs, Responsibilities of	10
Computer Direct-Access Authorization, Defined	4
Confidential Business Information, Defined	4
Contractor Security Requirements	6
Corrective Actions	
Discussed	29
Formal	30
Informal	29
Reassignment	30
Cover Sheet, Retaining	18
DAA/OTS, Responsibilities of	7
Department of Justice, Exemption for	28
Destruction	18
Director, MIDSD, Responsibilities of	8
Disciplinary Actions	
Formal	30
Informal	29
Division Directors, Responsibilities of	8
Document, Defined	5
Document Control Assistant, Defined	5
Document Control Assistants, Responsibilities of	11
Document Control Number, Defined	5
Document Control Officer, Defined	5
Document Control Officers Approved For Computer Access, Responsibilities of	10

Index (cont.)

	Page
Document Control Officers, Responsibilities of	9
Document Storage Rooms	13
Documents	
Lost	16
Generating and Classifying	18
Retiring of	18
Electronic Transmission	15, 24
Employee, Defined	15
Employees, EPA, Responsibilities of	11
Federal Agency, Defined	5
Forms, for Implementing Procedures	6
Generated Documents	18
Hardware Requirements, Computers	21
Information, Defined	5
Interagency Agreements	28
Investigations, Administrative, Full Field	4
Investigations, Background (NACI)	3
Logging Procedures	9
Logs, Retaining	18
Lost Documents	16
Mail, Incoming	15
Media	
Disposal of	24
Handling	24
Labeling	24
Transmittal of	24
Meetings	16
Notes	16
Office of the Inspector General, Responsibilities of	7
Penalties	
Administrative	2
Criminal	2
Photographs	18
Policy, EPA's CBI	1
Reassignment	32
Recovery Capability	25
Registered Mail	15
Regulations, Applicable to TSCA CBI	1

Index (cont.)

	Page
Reproduction	17
Retaining Logs	18
Retiring of Documents	18
Safeguards During Use of TSCA CBI	14
Secretarial Procedures	14
Secure Facility, Defined	5
Secure Room, Defined	5
Security Procedures, EPA, Individual Offices	6
Security Representative, Defined	5
Security Representatives, Responsibilities of	11
Security Requirements	
Contractor	6
Other Federal Agencies	27
Software System Design	19
Statutes, Applicable to TSCA CBI	1
Storage at EPA	13
Storage, Off-Site	25
Storage when Traveling	14
Submitter Representative, Defined	5
Telephone Calls	15
Transmission, Electronic	15, 24
Transmittal	
Outside an EPA Facility	17
Within an EPA Facility	17
Travel	14
Typing Procedures	14
Violations	
Defined	5
Other Federal Agencies	29
Suggested Penalties	31
Treatment of	1

*U.S. GOVERNMENT PRINTING OFFICE 341-082/256